UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,018	12/03/2003	David William Howell	GIL.P.US0030	7317

26360 7590 10/22/2007

RENNER KENNER GREIVE BOBAK TAYLOR & WEBER
FIRST NATIONAL TOWER FOURTH FLOOR
106 S. MAIN STREET
AKRON, OH 44308

EXAMINER	
JOHNS, CHRISTOPHER C	
ART UNIT	**PAPER NUMBER**
4172	

MAIL DATE	DELIVERY MODE
10/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/728,018	HOWELL, DAVID WILLIAM	
	Examiner	Art Unit	
	Christopher C. Johns	4172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 8, 12-14, and 17 rejected under 35 U.S.C. 102(b) as being anticipated by US Patent 5,251,259 (hereafter referred to as Mosley).

As per claim 1:

Mosley teaches a system for securing credit cards (and the like) by utilizing groups of PINs (Personal Identification Numbers) for each cardholder, using a different one for each transaction that a customer desires to make (cf. column 2, lines 23-28).

Mosley teaches using a card that has a grid of numbers and letters; the letters correspond to the day of the week that a purchase is made and the numbers correspond to the PINs used (cf. Figure 3 and column 2, lines 28-49 for an explanation of the system) (***1***: "*a data carrier for use by a card holder and separate from the transaction authorisation card, which data carrier has a list of transaction numbers and the corresponding unique codes for those numbers*"). When a cardholder wishes to make a purchase, the credit card is presented to a merchant and the correct PIN is provided to the vendor for entering into the system (cf. column 3, lines 4-12) (***1***: "*a local machine whereat a transaction is to be effected which local machine is able to communicate with the server over a data-link*"). If the given code is correct, the card company will allow the transaction. If the code is not correct, the card company will deny the transaction (cf. column 2, lines 26-28) (***1***: "*a server having stored therein a list, for each card holder intending to use a verification process running on the apparatus, of transaction numbers and for each such transaction number a respective unique code, the server running a programme for comparing the stored codes with a code to be supplied by a card holder on effecting a transaction*").

The customer gives the vendor a PIN based on the day and the number of transactions that have taken place that day (cf. column 5, lines 47-50) (***1***: "*whereby a card holder may effect a transaction at the local machine by using his authorisation card, the card holder also supplying to the local machine a transaction number and the unique code associated therewith for transmission to the server, the server comparing*

the supplied code with that stored in the server and allows or refuses the transaction dependent upon the result of that comparison").

As per claim 2:

In Mosley, it is mentioned that the credit card can be used at a "traditional retail or food establishment" which would include a conventional POS (point of sale) machine (cf. column 3, lines 4-12) (***2***: "*said local machine comprises a conventional point of sale card reading machine able to communicate with a centralised server*"). Additionally, this use is also inherent in the definition of a credit card.

As per claim 3:

Mosley mentions that the system is to be used as a way to "prevent charge and credit card fraud" (***3***: "*said transaction authorisation card comprises a conventional credit card or debit card*").

As per claim 4:

Mosley's system is used with credit cards, which inherently communicate data using phone lines (also, cf. claim 4) (***4***: "*said data-link comprises a conventional public telephone network service*").

As per claim 5:

The coding system in Mosley is written on a data carrier. See Figure 3; the system uses a grid to separate the identifying data from the actual PIN data. The days go along the top of the grid, and the PINs are picked from the center area of the grid. Further explanation of the exact method is contained from column 4, line 65 to column 5, line 39 (***5***: "*said data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area*").

As per claim 8:

Mosley teaches a system for securing credit cards (and the like) by utilizing groups of PINs (Personal Identification Numbers) for each cardholder, using a different one for each transaction that customer desires to make (cf. column 2, lines 23-28).

It uses a card that has a grid of numbers and letters; the letters correspond to the day of the week that a purchase is made and the numbers correspond to the PINs used

(cf. Figure 3 and column 2, lines 28-49 for an explanation of the system) (***8***: "*providing a card holder with a data carrier having a list of transaction numbers for that card holder and the corresponding unique codes for those numbers which codes are non-sequential on any given carrier*"). When a cardholder wishes to use the card, it is presented to a merchant and the correct PIN is provided to the vendor for entering into the system (cf. column 3, lines 4-12). If the given code is correct, the card company will allow the transaction. If the code is not correct, the card company will deny the transaction, since the company has a list of the approved PINs and a method for calculating the proper PIN based on day and number of transactions (cf. column 2, lines 26-28) (***8***: "*programming a server with a list, for each card holder who intends to use the method, of transaction numbers and for each such transaction number a respective unique code...whereafter the server allows or refuses the transaction dependent upon the result of a comparison of the transmitted code with that code programmed into the server*").

The customer gives the vendor a PIN based on the day and the number of transactions that have taken place (cf. column 5, lines 47-50) (***8***: "*the card holder effecting a transaction with the card; and the card holder being asked to specify a transaction number which number is transmitted to the server, the card holder also being asked for the unique code associated with that transaction number as read from the data carrier, which unique code is transmitted to the server*").

As per claim 12:

The server will permit a second attempt to use the card if the first entered PIN is incorrect (cf. column 6, lines 18-23) (***12***: "*the server permits at least a second attempt at verifying a transaction, in the event that the first attempt results in a refusal of the transaction.*").

As per claim 13:

In Mosley, it is mentioned that the credit card can be used at a "traditional retail or food establishment" which would include a conventional POS (point of sale) machine (cf. column 3, lines 4-12) (***13***: "*the server communicates with a vendor having control of a point of sale local machine and the vendor requests the relevant information from the card holder and acts as an intermediary between the card holder and the server.*"). Additionally, this use is also inherent in the definition of a credit card.

As per claim 14:

Mosley mentions that the system is to be used as a way to "prevent charge and credit card fraud" (***14***: "*the transaction authorisation card comprises one of a credit card or a debit card*").

As per claim 17:

The coding system in Mosley is written on a data carrier. See Figure 3; the system uses a grid to separate the identifying data from the actual PIN data. The days go along the top of the grid, and the PINs are picked from the center area of the grid. Further explanation of the exact method is contained from column 4, line 65 to column 5, line 39 (***5***: "*said data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area*", ***17***: "*data carrier for use in a verification procedure for a transaction by a card holder having a transaction authorisation card, which data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area*").

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6, 7, 9-11, 15, 18, and 19 rejected under 35 U.S.C. 103(a) as being unpatentable over Mosley.

As per claims 6 and 7:

Mosley teaches placing the PINs on the data carrier. Mosley does not teach covering the PINs with any sort of opaque covering to prevent others from seeing the PIN data.

The art of using opaque coverings over PIN data is well known in the art of phone cards (cf., for example, "Calling All Collectors: AT&T Introduces 2000 U.S. Olympic Series", paragraph 7) – the "original scratch-off" strip was well known to those

skilled in the art at the time of the invention to prevent the phone card from being used, since it hides the PIN from onlookers. Hiding the PIN from unauthorized users, whereby guaranteeing that the PIN is unused until the authorized cardholder decides to use it, was therefore well known in the art.

Phone cards and this invention both make a best effort to keep personal information secret – while this invention uses a grid along with a transaction number as well as other data, phone cards tend to use a scratch-off device. However, both systems will protect against unauthorized use of monetary instruments and attempt to notify the authorized user when a PIN has been used. Therefore, it would be obvious to one skilled in the art at the time of the invention to use the scratch-off material to cover the data carrier in Mosley, because of the desire to increase security and the guarantee to the user that the PIN has not yet been used (***6***: "*the unique codes of the data carrier are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom*", ***7***: "*the transaction numbers of the data carrier and associated with the unique codes are also covered with a strippable opaque coating, whereby the next transaction number and its associated code are together exposed when required for use*", ***18***: "*the unique codes are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom*", ***19***: "*the transaction numbers associated with the unique codes are also covered with a strippable opaque coating, whereby the next transaction number and its associated code are together exposed when required for use*").

As per claim 9:

It is not explicitly stated that the system in Mosley expires after a set amount of time. However, it was well known to those skilled in the art at the time of the invention to set expiration dates on credit cards to increase security. It would be natural, as well as obvious, to do the same thing for PIN data carriers – by expiring the carrier after a set amount of time, security is enhanced (***9***: "*the data carrier is valid for a limited period and is replaced periodically with a fresh supply of transaction numbers and corresponding unique codes*").

As per claim 10:

It would also be obvious to make the data carrier into a replaceable object – by preventing reuse of the PIN the card would become even more secure. However, employing one-time-use PINs was a security idea well known to those skilled in the art, as well as similar arts, at the time of the invention (cf., for example, US Patent 6,029,890, column 1, lines 26-32) (***10***: "*the data carrier is valid for only a specified number of transactions and is replaced with a fresh supply of transaction numbers and corresponding unique codes when that specified number of transactions has been effected*").

As per claim 11:

Well-known in the art of credit cards is the idea of "activation", whereby an authorized user must call the card company to confirm that the card has been properly received and the user is ready to charge items using it. The Examiner takes Official Notice that activating such cards is essential to their use, and that activation of cards was well known to those skilled in the art at the time of the invention.

While Mosley does not explicitly state that the card containing PIN information must be activated, it would be obvious to one skilled in the art at the time of the invention to require users to activate the PIN card upon receipt – just as with the credit card, knowledge that the authorized user has received the card is essential to credit card security, which is the ultimate aim of this invention (***11***: "*the data carrier must be activated following receipt thereof by a card holder, before the data carrier may be employed to verify transactions*").

As per claim 15:

It is not explicitly stated that the system in Mosley expires after a set amount of time. However, it was well known to those skilled in the art at the time of the invention to set expiration dates on credit cards to increase security. It would be natural, as well as obvious, to do the same thing for PIN data carriers – by expiring the carrier and giving the customer a new one after a set amount of time, security is enhanced (***15***: "*a fresh data carrier is supplied to the card holder with a statement of transactions effected over a previous period*").

As per claims 18 and 19:

Mosley teaches placing the PINs on the data carrier. Mosley does not teach covering the PINs with any sort of opaque covering to prevent others from seeing the PIN data.

The art of using opaque coverings over PIN data is well known in the art of phone cards (cf., for example, "Calling All Collectors: AT&T Introduces 2000 U.S. Olympic Series", paragraph 7) – the "original scratch-off" strip was well known to those skilled in the art at the time of the invention to prevent the phone card from being used, since it hides the PIN from onlookers. Hiding the PIN from unauthorized users, whereby guaranteeing that the PIN is unused until the authorized cardholder decides to use it, was therefore well known in the art.

Phone cards and this invention both make a best effort to keep personal information secret – while this invention uses a grid along with a transaction number as well as other data, phone cards tend to use a scratch-off device. However, both systems will protect against unauthorized use of monetary instruments and attempt to notify the

authorized user when a PIN has been used. Therefore, it would be obvious to one skilled in the art at the time of the invention to use the scratch-off material to cover the data carrier in Mosley, because of the desire to increase security and the guarantee to the user that the PIN has not yet been used (***18***: "*the unique codes are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom*", ***19***: "*the transaction numbers associated with the unique codes are also covered with a strippable opaque coating, whereby the next transaction number and its associated code are together exposed when required for use*").

Claims 1-10, 12, and 14-19 rejected under 35 U.S.C. 103(a) as being unpatentable over OTPW, a One-Time Password login package created by Markus Kuhn..

As per claims 1-4:

OTPW is a system for securing logins to computer systems using one-time passwords that a user must carry on a sheet (cf. "How it works", 4th paragraph – the user is asked to print the sheet out and keep it) (***1***: "*a data carrier for use by a card holder and separate from the transaction authorisation card, which data carrier has a list of transaction numbers and the corresponding unique codes for those numbers*"). Users use the password on their local machine in order to log into a remote one (cf. "Introduction", 2nd paragraph) (***1***: "*a local machine whereat a transaction is to be effected which local machine is able to communicate with the server over a data-link*") – a unique password is used along with a password number (cf. "How it works", 6th paragraph, and 3rd paragraph – the passwords are listed with password numbers) (***1***: "*whereby a card holder may effect a transaction at the local machine by using his authorisation card, the card holder also supplying to the local machine a transaction number and the unique code associated therewith for transmission to the server, the server comparing the supplied code with that stored in the server and allows or refuses the transaction dependent upon the result of that comparison*"). The usable passwords are generated on the remote machine for use with the program (cf. "How it works", 1st and 2nd paragraph) (***1***: "*server having stored therein a list, for each card holder intending to use a verification process running on the apparatus, of transaction numbers and for each such transaction number a respective unique code, the server running a programme for comparing the stored codes with a code to be supplied by a card holder on effecting a transaction*").

The system is used for computer logins. The system does not purport to be a solution for credit card systems. However, the usage of one-time-use PINs to secure credit card transactions was well known to those skilled in the art at the time of the invention (cf., for example US Patent 6,029,890, column 1, lines 26-32). Therefore, it

would have been obvious to one skilled in the art at the time of the invention to use the paradigm in OTPW to achieve a one-time-use PIN for credit card systems, since it is one of many one-time-use password systems, and both types of systems attempt to keep out unauthorized users and protect personal information (***2***: "*said local machine comprises a conventional point of sale card reading machine able to communicate with a centralised server*", ***3***: "*said transaction authorisation card comprises a conventional credit card or debit card*", ***4***: "*said data-link comprises a conventional public telephone network service*").

As per claim 5:

The passwords, according to OTPW, are listed in table format. Each entry of the password table contains a password number and the corresponding password (cf. "How it works", 2nd paragraph and enclosed table) (***5***: "*said data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area*").

As per claims 6 and 7:

The art of using opaque coverings over personal data is well known in the art of phone cards (cf., for example, "Calling All Collectors: AT&T Introduces 2000 U.S. Olympic Series", paragraph 7) – the "original scratch-off" strip was well known to those skilled in the art at the time of the invention to prevent the phone card from being used, since it hides the PIN from onlookers. Hiding the PIN from unauthorized users, whereby guaranteeing that the PIN is unused until the authorized cardholder decides to use it, was therefore well known in the art.

Phone cards and OTPW both make a best effort to keep personal information secret – while this invention uses a grid along with a transaction number as well as other data, phone cards tend to use a scratch-off device. However, both systems will protect against unauthorized use of personal data and attempt to notify the authorized user when a PIN has been used (if a PIN has been used, it will not be asked for again – additionally, in the case of a concurrent login attack, three passwords will be asked for – cf. "How it works", 6th paragraph). Therefore, it would be obvious to one skilled in the art at the time of the invention to use the scratch-off material to cover the data carrier in OTPW, because of the desire to increase security and the guarantee to the user that the PIN has not yet been used (***6***: "*the unique codes of the data carrier are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom*", ***7***: "*the transaction numbers of the data carrier and associated with the unique codes are also covered with a strippable opaque coating,*

whereby the next transaction number and its associated code are together exposed when required for use").

As per claims 8 and 14:

OTPW is a system for securing logins to computer systems using one-time passwords that a user must carry on a sheet (cf. "How it works", 4th paragraph – the user is asked to print the sheet out and keep it) (***8***: "*providing a card holder with a data carrier having a list of transaction numbers for that card holder and the corresponding unique codes for those numbers which codes are non-sequential on any given carrier*"). Users use the password on their local machine in order to log into a remote one (cf. "Introduction", 2nd paragraph) – a unique password is used along with a password number (cf. "How it works", 6th paragraph, and 3rd paragraph – the passwords are listed with password numbers) (***8***: "*the card holder effecting a transaction with the card; and the card holder being asked to specify a transaction number which number is transmitted to the server, the card holder also being asked for the unique code associated with that transaction number as read from the data carrier, which unique code is transmitted to the server; whereafter the server allows or refuses the transaction dependent upon the result of a comparison of the transmitted code with that code programmed into the server*"). The usable passwords are generated on the remote machine for use with the program (cf. "How it works", 1st and 2nd paragraph) (***8***: "*programming a server with a list, for each card holder who intends to use the method, of transaction numbers and for each such transaction number a respective unique code*").

The system is used for computer logins. The system does not purport to be a solution for credit card systems. However, the usage of one-time-use PINs to secure credit card transactions was well known to those skilled in the art at the time of the invention (cf., for example US Patent 6,029,890, column 1, lines 26-32). Therefore, it would have been obvious to one skilled in the art at the time of the invention to use the paradigm in OTPW to achieve a one-time-use PIN for credit card systems, since it is one of many one-time-use password systems, and both types of systems attempt to keep out unauthorized users and protect personal information (***14***: "*the transaction authorisation card comprises one of a credit card or a debit card*").

As per claims 9, 10:

The sheet of paper containing passwords is only valid for a certain number of logins – after a password is used it is no longer valid (inherent to the definition of a one-time password scheme). Therefore, the sheet will have to be replaced every so often (***9***: "*the data carrier is valid for a limited period and is replaced periodically with a fresh supply of transaction numbers and corresponding unique codes*", ***10***: "*the data carrier is valid for only a specified number of transactions and is replaced with a fresh supply of*

transaction numbers and corresponding unique codes when that specified number of transactions has been effected").

As per claim 12:

Inherent to the definition of a login attempt is the ability to try again if the entered password is not correct. If a user mistypes a password, the user may attempt to log in again (***12***: "*the server permits at least a second attempt at verifying a transaction, in the event that the first attempt results in a refusal of the transaction.*")

As per claim 16:

The server generates the password number requested and sends it to the user upon an attempt to log in (cf. "How it works", 5th paragraph with login screen reproduction) (***16***: "*the server generates the transaction number to be used to verify a transaction and returns that transaction number to the card holder so that the card holder may supply the server with the corresponding unique code from the data carrier, for verification*").

As per claim 17:

The passwords, according to OTPW, are listed in table format. Each entry of the password table contains a password number and the corresponding password (cf. "How it works", 2nd paragraph and enclosed table) (***17***: "*data carrier for use in a verification procedure for a transaction by a card holder having a transaction authorisation card, which data carrier has a first data area and a second data area, the first data area having a plurality of transaction numbers marked thereon which numbers change incrementally, and the second data area having a plurality of unique codes marked thereon, one such code being associated with each transaction number respectively, whereby for a given transaction number a corresponding unique code may be read off the second data area*").

As per claims 18 and 19:

The art of using opaque coverings over personal data is well known in the art of phone cards (cf., for example, "Calling All Collectors: AT&T Introduces 2000 U.S. Olympic Series", paragraph 7) – the "original scratch-off" strip was well known to those skilled in the art at the time of the invention to prevent the phone card from being used, since it hides the PIN from onlookers. Hiding the PIN from unauthorized users, whereby guaranteeing that the PIN is unused until the authorized cardholder decides to use it, was therefore well known in the art.

Phone cards and OTPW both make a best effort to keep personal information secret – while this invention uses a grid along with a transaction number as well as

other data, phone cards tend to use a scratch-off device. However, both systems will protect against unauthorized use of personal data and attempt to notify the authorized user when a PIN has been used (if a PIN has been used, it will not be asked for again – additionally, in the case of a concurrent login attack, three passwords will be asked for – cf. "How it works", 6th paragraph). Therefore, it would be obvious to one skilled in the art at the time of the invention to use the scratch-off material to cover the data carrier in OTPW, because of the desire to increase security and the guarantee to the user that the PIN has not yet been used (***18***: "*the unique codes are covered with a strippable opaque coating, whereby each unique code may be exposed by removing the strippable coating therefrom*", ***19***: "*the transaction numbers associated with the unique codes are also covered with a strippable opaque coating, whereby the next transaction number and its associated code are together exposed when required for use*").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher C. Johns whose telephone number is 571-270-3462. The examiner can normally be reached on Monday-Thursday, 7:30-5, Alternate Fridays, 7:30-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tom Dixon can be reached on 571-272-6803. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christopher Johns
Examiner
Art Unit 4172

CCJ

THOMAS A. DIXON
SUPERVISORY PATENT EXAMINER